Formal Development and Verification of Safe Railway Control Systems

Haxthausen, Anne Elisabeth

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

DTU Compute
Department of Applied Mathematics and Computer Science

RobustRailS

Formal Development and Verification of Safe Railway Control Systems

Research Question

Before 2021 all Danish signalling systems are going to be replaced with modern computer based systems. Central parts of these systems consist of *safety-critical software*.

Challenges: How to develop such new systems *efficiently* (i.e. cheap and fast) and at the same time ensure that they are *safe*?

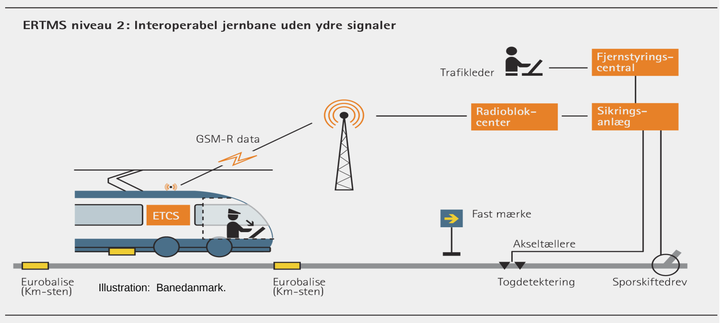


Illustration: Banedanmark.

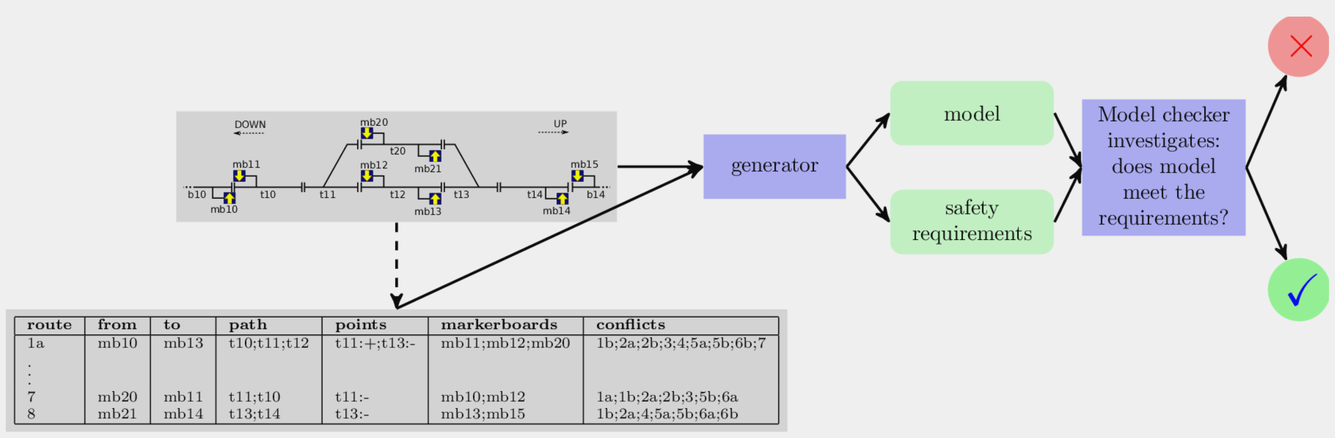
Research Goals of RobustRailS WP 4.1

Goals: to provide efficient methods and tools for the development and safety verification of such systems.

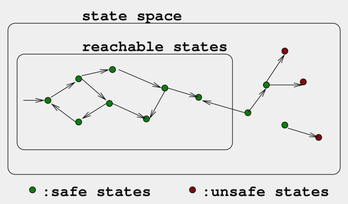
The **main approach** to achieve this is to make use of *automation* and *formal (mathematically based) methods*, as formal methods are strongly recommended by the CENELEC 50128 standard.

Case Study: Safety Verification of ERTMS/ETCS Level 2 Based Interlocking Systems

A tool chain for verifying control algorithms and train route control tables:



route	from	to	path	points	markerboards	conflicts
1a	mb10	mb13	t10;t11;t12	t11:+;t13:-	mb11;mb12;mb20	1b;2a;2b;3;4;5a;5b;6b;7
.						
.						
.						
7	mb20	mb11	t11;t10	t11:-	mb10;mb12	1a;1b;2a;2b;3;5b;6a
8	mb21	mb14	t13;t14	t13:-	mb13;mb15	1b;2a;4;5a;5b;6a;6b



A model

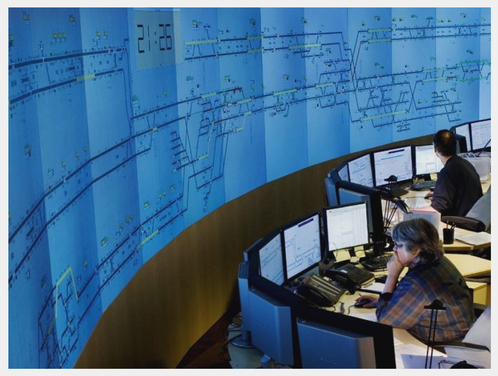
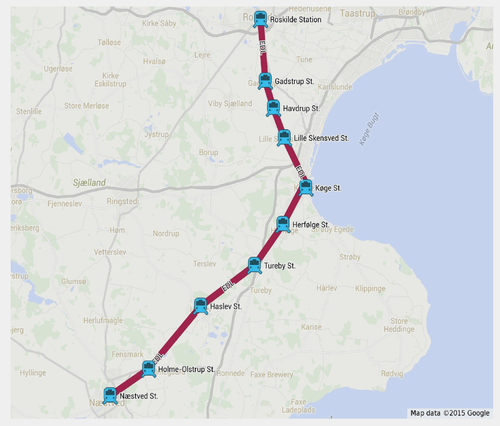


Foto: Banedanmark

Method:

1. An interlocking system is specified by a *track plan* and a *train route control table*.
2. The *train route control table* can be *automatically generated* from the track plan.
3. A tool *automatically verifies* the specification for a number of correctness properties.
4. A tool *automatically generates*
   (a) a *formal model* of all possible behaviours of the interlocking system and
   (b) *formal safety requirements* (e.g no train collisions + no derailments).
5. A model checker *automatically proves* that the *model* satisfies *the safety requirements*.

   The proof is made combining advanced mathematical techniques and SMT solving.



Early deployment line East

Experiments:

The method has successfully been applied to the early deployment line in East Denmark.

RobustRailS
Assoc. Professor Anne Haxthausen (aeha@dtu.dk)
The Railway Verification Group at DTU Compute
For more info, see http://www.imm.dtu.dk/~aeha/Railway

banedanmark
InnovationsFonden
FORSKNING, TEKNOLOGI & VÆKST I DANMARK
Universität Bremen
DTU